User Guide
IP Connect CSD

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing.
Wireless Maingate AB shall have no liability for any error or damages of any kind resulting from use of this document.

Revision: 1.0

maingate

ADDRESS: BOX 244, SE-371 24 KARLSKRONA, SWEDEN
VISITORS: DROTTNINGGATAN 16
PHONE. +46 455 36 37 00 FAX: +46 456 36 37 37
WEB: WWW.MAINGATE.SE

Table of Contents

1	Introduction	3
2	Service overview	3
2.1	Service specification	3
2.2	Terminal requirements	3
3	Device IP ranges	4
4	IP network configuration	5
4.1	VPN configuration	5
4.2	IP routing	5
4.3	Firewall configuration	6
5	Registering terminals	7
6	Communication	9
6.1	Access numbers	9
6.2	Addressing terminals	9
6.3	Terminal-initiated connection	10
6.4	Application-initiated connection	11
6.5	Disconnection	11
6.6	Connection duration	11
6.7	Capacity	11
7	Appendix – scripts	12
7.1	LSD0-V110	12
7.2	LSD0-V32	12
7.3	Terminology	12

1 Introduction

This document is intended to be used by the customer during configuration and use of the Maingate IP Connect CSD service.

2 Service overview

IP Connect CSD provides transparent TCP/IP communication between a customer application and terminals equipped with GSM or PSTN modems. An overview of the functionality is shown in Figure 1.

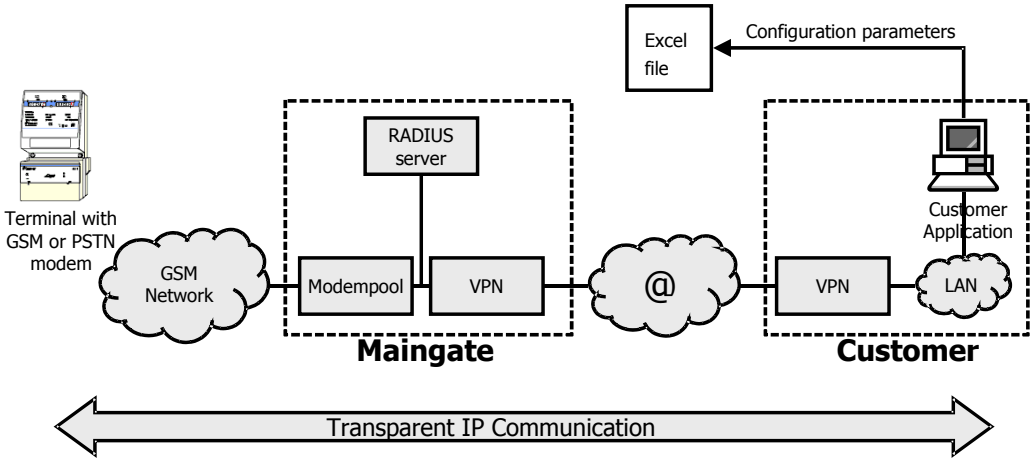

Figure 1 – Service overview

The customer application is connected to Maingate over Internet using a VPN tunnel. Each terminal is configured once in Maingate's RADIUS with desired parameters that controls the communication settings, through an XML API. Once the configuration has been done, communication is initiated by sending an IP packet from application or from a terminal by making a PPP connection.

2.1 Service specification

The Maingate IP Connect CSD service supports the following functionality:

- Support for IP addressing according to IP v4

2.2 Terminal requirements

In order for the IP Connect CSD service to be successfully used with a terminal, the terminal must satisfy the following requirements:

- The terminal must support PPP according to RPC 1661 of the IETF
- The terminal must use Default Route during PPP connection

- The terminal must support dynamic IP address allocation over PPP

3 Device IP ranges

Since a terminal is identified and addressed using its IP address, it is vital to secure that each terminal always is allocated a unique IP address. IP Connect CSD performs a check each time a terminal is registered to verify that the IP address is unique.

In order to avoid that different IP Connect CSD accounts attempt to associate the same IP address to different terminals, each account is only permitted to register IP addresses from a predefined number of IP address ranges. These IP address ranges are compared and verified during service ordering.

Note!	If one IP Connect CSD account has been allocated a certain range of IP addresses, this range cannot be used by another account. This is the reason why Maingate reserves the right to refuse the use of certain IP addresses.

It is possible allocate several IP address ranges to one IP Connect CSD account. IP address ranges may be allocated from both public as well as private IP address areas.

In addition to the first (subnet address) and the last (broadcast address) address of each subnet, the second address is reserved for internal purposes. Thus the usable range of addresses in each subnet always excludes these three addresses. An example of an allocated range is shown in Table 1.

Subnet	150.150.150.0
Mask	255.255.255.0
Nominal range	150.150.150.0 to 150.150.150.255
Usable range	150.150.150.2 to 150.150.150.254

Table 1 – Example of IP range definition

4 IP network configuration

In order for IP Connect CSD to function correctly, the transmission of IP packets between Maingate and the customer must be carefully configured. A VPN tunnel is used to carry the traffic between terminals and application. The VPN tunnel ensures that private IP addresses can be used protects data across the Internet and ensures that one customer's traffic is separated from other traffic.

4.1 VPN configuration

IPSec encryption is used for the VPN tunnel between Maingate and the LAN connecting the customer application. IPSec is a set of standard protocols for implementing secure communications and encryption key exchange between computers.

An IPSec VPN generally consists of two communication channels between the endpoint hosts: a key-exchange channel over which authentication and encryption key information is passed, and one or more data channels over which private network traffic is carried.

The key-exchange channel is a standard UDP connection to and from port 500. The data channels carrying the traffic between the client and server use IP protocol number 50 (ESP).

More information is available in RFC 2402 (the AH protocol, IP protocol number 51), RFC 2406 (the ESP protocol, IP protocol number 50), and RFC 2408 (the ISAKMP key-exchange protocol).

Configuration details are provided by mail form Maingate after service ordering.

4.2 IP routing

Once the VPN tunnel has been established, the customer LAN must be configured to route applicable packets through the VPN and allow packets from the VPN to reach the customer application.

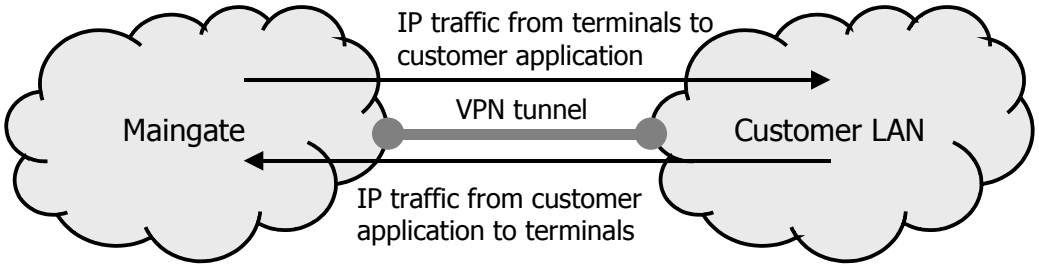

Figure 2 –IP routing between Maingate and customer LAN

The VPN tunnel is only used for data traffic between terminals and application.

4.3 Firewall configuration

The customer must secure that the customer's firewall is open to allow the types of IP sessions to pass that are used by terminal and application. If not, the IP packets will be blocked by the customer's firewall and communication will not function correctly. Maingate firewall towards the VPN tunnel is open to allow for all types of IP sessions to pass.

5 Registering terminals

Before communication can take place, each terminal must be registered at Maingate. Customers can create a “comma separated values” file (.csv) and send it to Maingate for registration. Registration of Mobile Originating (MO)- and Mobile Terminating (MT) users require two separate files.
Customer can use IP connect CSD for MO- or MT traffic only or both.

Below the required parameters for MO- and MT users respectively is explained.

Parameters for MO:

UserName	This parameter is used for authentication as login ID for terminal-initiated connections. UserName also uniquely identifies the terminal in RADIUS. Thus, two terminals may not be assigned the same UserName.
Password	This parameter is used for authentication as password for terminal-initiated connections.
IP	This parameter is the IP address that is used to connect to a terminal for application-initiated connections and the IP address that identifies a terminal in the customer application for terminal-initiated connections. IP must be unique for each terminal.

Note! The parameters UserName, MSISDN and IP must always be unique for each registered terminal.

Parameters for MT:

UserName	This parameter is used for authentication as login ID for application-initiated connections.
Password	This parameter is used for authentication as password for application-initiated connections.
MSISDN	This parameter is the telephone or mobile number of the terminal. MSISDN must be unique for each terminal.
IP	This parameter is the IP address that is used to connect to a terminal for application-initiated connections and the IP address that identifies a terminal in the customer application for terminal-initiated connections. IP must be unique for each terminal.

IdleTime	This parameter defines the maximum idle time for connections in minutes. If no IP packets are sent between application and terminal during this period of time, IP Connect will terminate the connection.
Script	This parameter defines what communication parameters are used for communication to a terminal. Communication parameters are defined in groups (scripts), each with a unique name. The available scripts are presented in Appendix – scripts.
Authentication	This parameter defines the authentication type that is used for the terminal. Possible values are PAP, CHAP or no authentication.

6 Communication

After a terminal has been registered in RADIUS, it is possible to initiate IP communication to and from that terminal.

6.1 Access numbers

A connection between terminal and customer application may be initiated either by a terminal or by the customer application.

For terminal-initiated connections, the terminal dials one of Maingates access numbers. The available access numbers are detailed in the service confirmation that is sent to the customer.

For application-initiated connections, the application sends an IP packet through the VPN tunnel to Maingate. The packet is always routed in the same way regardless of where the terminal is located. Figure 3 describes the routing between access numbers and VPN.

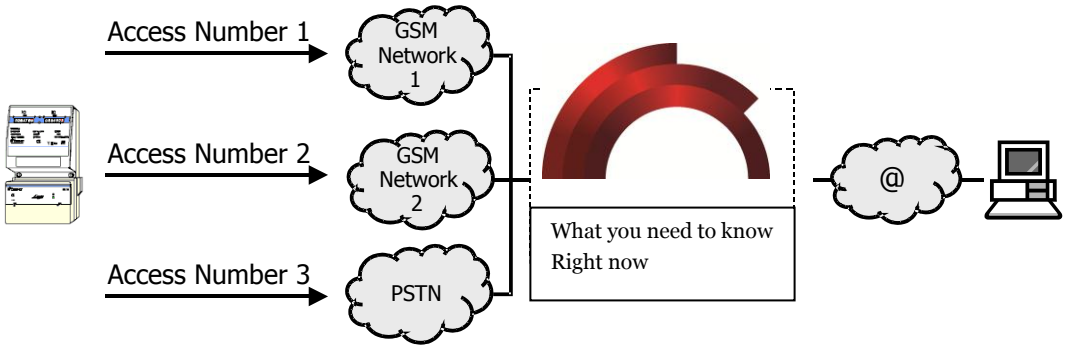

Figure 3 – Access numbers in different networks

6.2 Addressing terminals

For application-initiated connections, the IP address uniquely identifies what terminal is to be connected to. For terminal-initiated connections, the UserName parameter uniquely identifies the terminal and provides the mapping to the correct IP address which identifies the terminal to the customer application.

The terminal must be configured to accept a dynamic IP address. The mapping of parameters for terminal-initiated and application-initiated connection is shown in Figure 5 and Figure 6.

Note!	Even though the terminals use dynamic IP address allocation over PPP, the terminal will always be assigned the same IP address (which has been configured through the XML API) from RADIUS for each session.

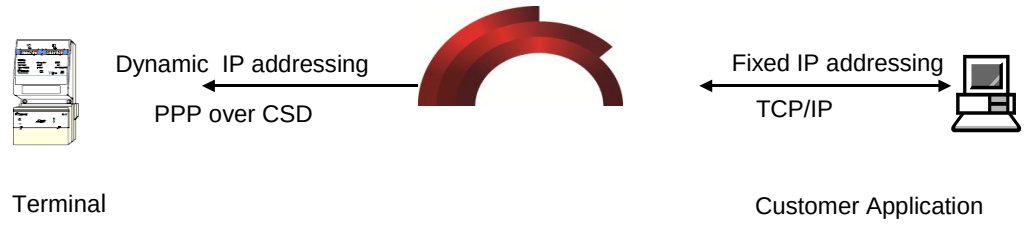

Figure 4 – IP address allocation

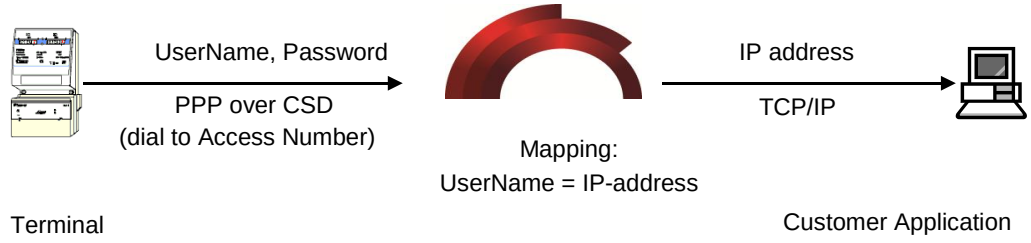

Figure 5 – Parameter mapping for terminal-initiated connection

Figure 6– Parameter mapping for application-initiated connection

6.3 Terminal-initiated connection

To initiate communication from a terminal, the terminal dials one of the Access Numbers. The access server will answer the call and start protocol negotiation, authentication and IP address negotiation. The terminal's UserName serves as the identification key to identify what terminal is requesting communication.

Communication is set-up through protocol negotiation between terminal and access server. Authentication is performed by comparing parameters supplied by the terminal with UserName and Password stored in RADIUS.

Once the PPP session has been successfully initiated, IP packets can be transmitted between terminal and application transparently.

6.4 Application-initiated connection

To initiate communication from the customer application, the customer application sends a TCP packet addressed to the desired terminal through the VPN tunnel to Maingate. Using the destination IP address as a key, the correct terminal is identified in RADIUS. The access server dials the terminal using the correct MSISDN and starts protocol negotiation, authentication and IP address negotiation.

Note!	Only a TCP type packet will initiate a session to the terminal. Sending other types of packets will not initiate a session. Once the session is established, other packet types can be transmitted.

Protocol negotiation between terminal and access server is done according to the script that has been configured for the specific terminal. Authentication is performed by comparing parameters UserName and Password, stored in RADIUS, with the parameters in the terminal.
Once the PPP session has been successfully initiated, IP packets can be transmitted between terminal and application transparently.

6.5 Disconnection

Disconnection of the session can be performed by the terminal by disconnection of the CSD call. Alternatively, IP Connect CSD will disconnect the session if no IP packets have been transmitted between terminal and customer application for more than the configured Idle Time.

Note!	Only a TCP type packet will reset the idle timer. Thus, if other packet types are transmitted, this will not be recognised as valid traffic, resulting in a potential disconnection of the session.

6.6 Connection duration

During the set-up of the PPP session, the first IP packet from the terminal or application is buffered during session set-up. The duration of this initial transfer delay is typically between 10 to 15 seconds, and normally never more than 30 seconds. After initial PPP set-up, subsequent packets are transferred according to the available communication speed in the GSM network.

Note!	The application in the terminal and the customer application must be designed to allow for the initial transfer delay.

6.7 Capacity

The available communication capacity is defined in terms of simultaneous CSD connections per IP Connect account. IP Connect CSD will not allow additional connections to be established if the maximum number is already being used. If a terminal attempts to initiate an additional connection when the used capacity is at a maximum, the access server will disconnect the call. If the customer application attempts to initiate an additional connection when the used capacity is at a maximum, the IP packet will be refused.

Additional capacity to an existing account can be ordered by contacting Maingate Support.

7 Appendix – scripts

The following scripts are supported:

7.1 LSDO-V110

Parameter	Description	Setting
Modulation Standard		V.110

7.2 LSDO-V32

Parameter	Description	Setting
V.42 Detect Phase		Disabled
Data Compression		Disabled
V.42 LAP-M Error Correction		Disabled
MNP Error Correction		Disabled
Modulation Standard		V.32bis, V.32 V.23 V.22bis, V.22 V.21 BELL212 BELL103
Maximum Connect Rate		9600 bps
V.8bis Capacity		Disabled

7.3 Terminology

Access Number	Telephone number in GSM or PSTN to which terminals can dial in to make connection
Account	An IP Connect account containing a group of terminals and a customer application between which communications can take place
API	Application Programming Interface
CHAP	Challenge Authentication Protocol
CSD	Circuit-Switched Data
GSM	Global System for Mobile communication
IP Default Route	Default destination of unspecified IP packets

LAN	Local Area Network
PAP	Password Authentication Protocol
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-in User Service
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
XML	Extensible Mark-up Language